Tema 1: Arquitecturas de Comunicaciones.

1. Introducción: Conceptos Preliminares.

- **RED:** Elemento abstracto que nos permite conectar equipos entre sí. Lo importante en una red es como encaminamos la información.

  Podemos clasificar las redes basándonos en su aspecto:

  - **REDES DE COMUNICACIÓN:** Redes físicas que engloban cualquier tipo de red existente y servicios de comunicaciones.
  - **REDES DE COMPUTADORES:** Redes lógicas, abstractas formadas mediante redes de comunicación y basadas en:
    1. Mismo direccionamiento
    2. Conjunto de protocolos que permiten comunicar dos maquinas.

- **INTERNET:** Conexión de redes con distintas tecnologías (Físicas + Lógicas) interconectadas por routers.

  Utiliza lenguaje IP: Se usa para encaminar la información con independencia de cómo este implementado por debajo.

- **ARQUITECTURA DE COMUNICACION:** Conjunto de reglas capaz de comunicar distintos equipos.

  Se dividen en distintos niveles que van a dar distintos servicios. El número de niveles van a depender de la independencia que queramos.

- **ESTANDARES DE PROTOCOLOS:**

  - **PROTOCOLO:** Conjunto de reglas mediantes las cuales se pueden comunicar dos maquinas (emisor, receptor). Estas reglas sirven para evitar colisiones, control de acceso, control de encaminamiento,…
  - **ESTANDARIZAR:** Consiste en definir, proponer, aprobar y publicar los protocolos estratificados en estándares.

    Existen dos tipos de estándares:

    * **DE IURE:** Formal, etéreo como OSI de ISO que primero se estandarizo y luego se implemento.
    * **DE FACTO:** TCP/IP. Se tiene la idea, se implementa y si funciona se estandariza.

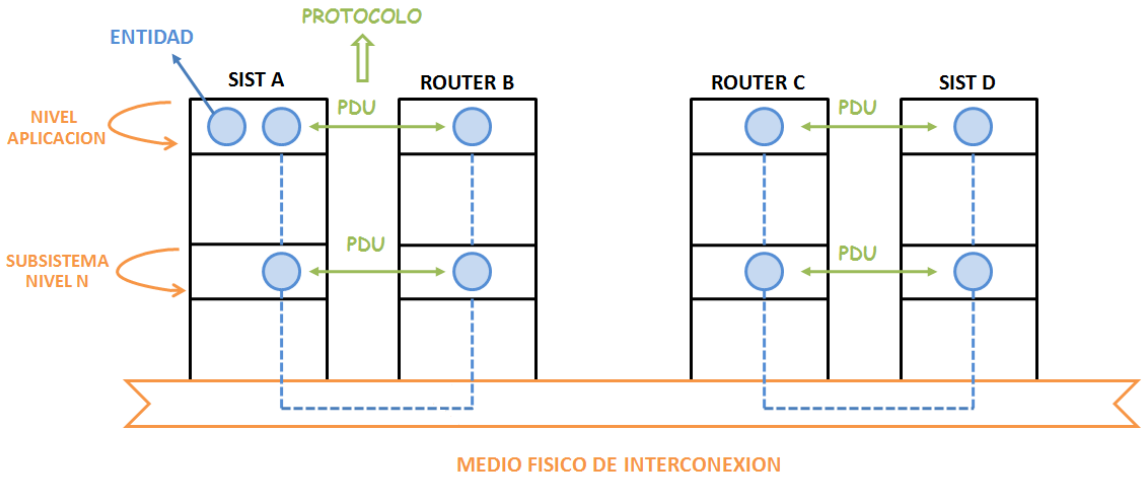
2. Estratificacion en Niveles.

- **VENTAJAS:**

  - **REDUCCION DE COMPLEJIDAD:** Facilita la labor de diseño. Tiene una estructura más comprensible dividiendo en diferentes niveles de comunicación mutuamente independientes.

    Diferentes equipos en distintos niveles, es decir, si tenemos funcionalidades parecidas se pueden tratar en distintos niveles y en distintos ámbitos.

  - **FACILITA EL CAMBIO TECNOLOGICO:** Cualquier cambio llevado a cabo en un nivel no afecta al resto de los niveles de la arquitectura ya que son independientes.



La referencia estandarizada para la descripción conceptual de los niveles de comunicaciones de otras arquitecturas => MODELO OSI (ISO/IEC IS 7498-1)

Las comunicaciones se producen a través de un medio físico (cable) y se producen entre el sistema A y el sistema D; que se encuentran conectados mediante los routers B y C.

- **ROUTERS:** Encaminan datos entre dos equipos, pero solo ofrecen funcionalidades a los niveles superiores.

Un nivel inferior da un servicio a una capa superior, que solo va a poder ver su interfaz.

- **INTERFAZ:** Funciones que el nivel inferior ofrece al nivel superior. No tiene porque estar estandarizados.

Podemos establecer dos niveles de comunicación:

1. Entre distintos niveles
2. Entre entidades mediante un protocolo común que debe estar estandarizado.

Un nivel puede tener más de una entidad. Cada nivel tiene uno o varios protocolos, uno por cada entidad que tiene el nivel.

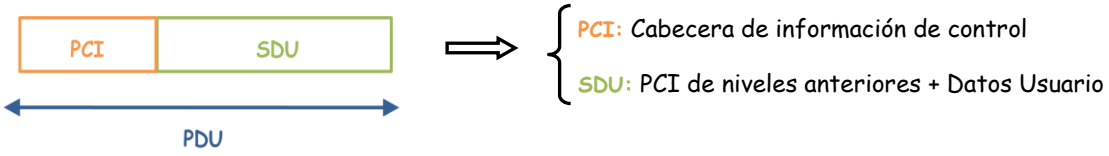
* **NIVEL IP:** Solo tiene entidad IP (en principio).
* **NIVEL TRANSPORTE:** Tiene dos entidades, esto implica dos protocolos distintos: TCP y UDP.

Los niveles inferiores son los que más relación tienen con la red física.

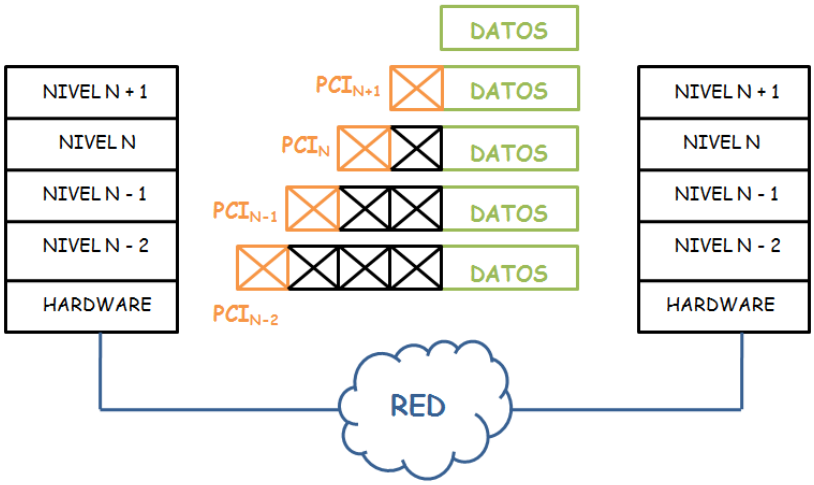
- **ENTIDAD:** Software de comunicación IP en el router y en el destino, además codifica el protocolo que tiene que seguir el software de comunicaciones.
  - **ENTIDADES HOMOLOGAS/PARES:** Tienen el mismo protocolo en cada extremo. Tienen que tener interfaces estandarizadas.
    Niveles adyacentes tienen entidades pares para poder enviarse información.
- **PDU:** Unidad de datos de Protocolo. Paquete de datos o también llamado paquete IP. Es la información que queremos enviar.

Para diferenciar dos PDU'S nos tenemos que fijar en su cabecera (lo único en lo que se diferencian).

- **FORMATO:**



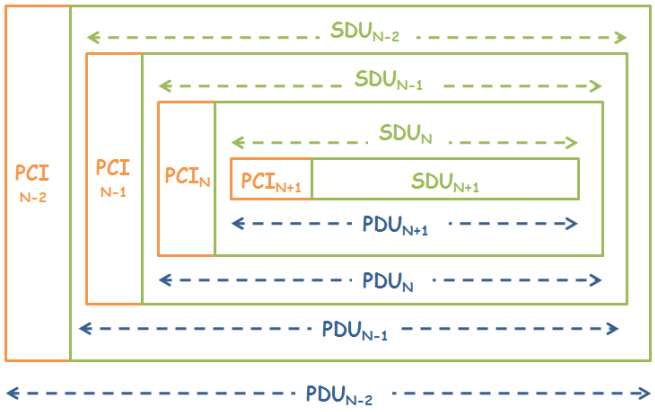
Cada nivel añadirá su propia cabecera: entre distintos niveles las cabeceras no tienen sentido. Aunque hayan mas cabeceras cada nivel solo va a entender la cabecera de su homologo.

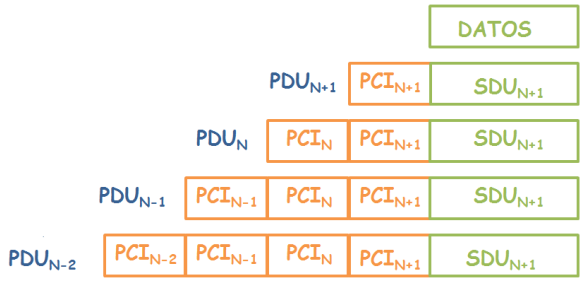


Esta estructura dibujada en la figura es compartida tanto por emisor como por receptor pero las PCI'S y los datos son distintos para cada uno de ellos (solo comparten el formato de representación).

Un nivel no puede ni mirar, ni tocar, ni interpretar los datos que no pertenecen a su nivel, para saber si pertenecen a o no a su nivel miran la cabecera de los datos transferidos.

- **ENCAPSULACIÓN DE PDU'S:** La PDU de un nivel es la PCI del nivel mas la SDU del nivel superior. (SDU ≡ unidad de datos del servicio).



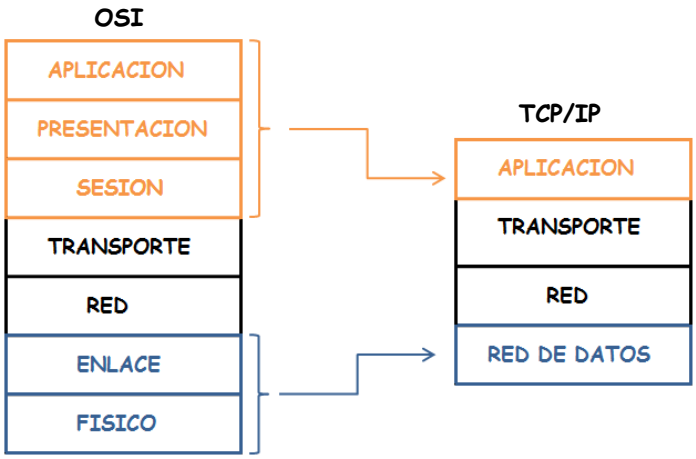


$PDU_{N-1} = PCI_{N-1} + PDU_N$

$SDU_N = PDU_{N+1} \Rightarrow PDU_N = SDU_{N-1}$

3. Modelo OSI de ISO.

El OSI es un modelo teórico, actualmente el modelo que se usa es el TCP/IP.



- **FISICO (NIVEL 1):** Da acceso al soporte de transmisión.

  Se encarga del envío de datos a través del medio físico. En él se encuentran los protocolos.

  No es importante en la informática.

  Su PDU no tiene nombre, porque actúa a nivel de bit.

- **ENLACE (NIVEL 2):** Se encarga del intercambio de datos entre dos entidades contiguas. Realiza encaminamiento local.

  A su PDU se le llama **TRAMA** ⇒ Datos que se envían.

  En este nivel se produce control de flujo y control de errores.

  Se usa un protocolo fiable (con control de errores)

El valor de una red crece con el número de usuarios que la usan, hasta cierto punto en el que se podría saturar.

- **RED (NIVEL 3):** Permite realizar encaminamiento de manera global, es decir, encaminar hacia distintas redes.

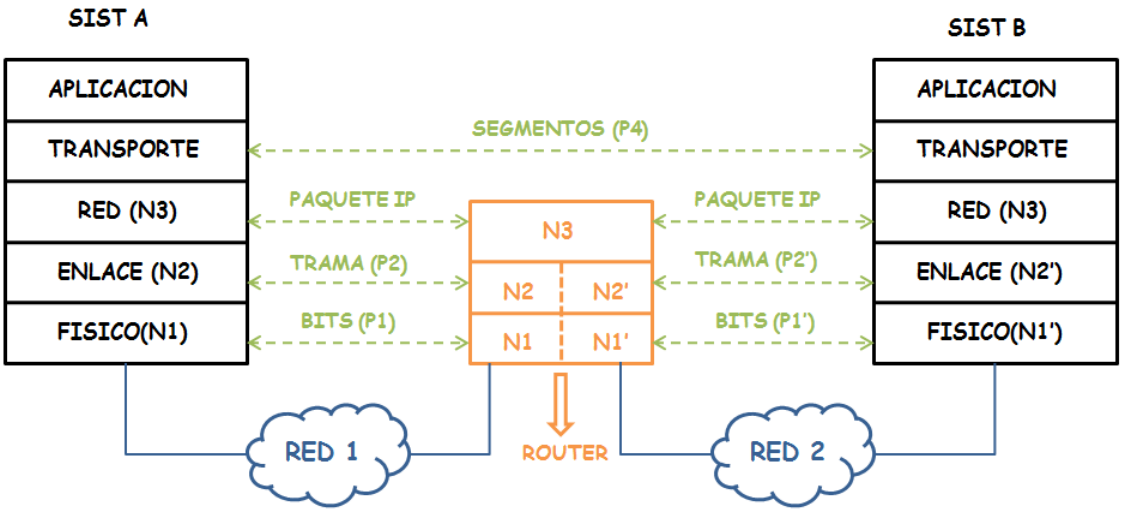
  Permite hablar de redes abstractas interconectadas por un router. Se abstrae del nivel tecnológico.

  La PDU de este nivel se denomina **PAQUETE** o **DATAGRAMA IP**.

  Se utiliza un protocolo IP que no es fiable. Si por la red se modifica algún bit, el destino descarta el paquete. Solo se mira la cabecera del paquete, si tiene errores en la cabecera se descarta pero si los errores solo están el cuerpo del paquete, éste se enviara y tendrá que solucionar el error algún nivel superior.

  El no tener ningún control es debido a que el router (que es el que mira los errores) tiene que funcionar muy rápido y con poco consumo.

  Si un router se satura descarta los paquetes que le lleguen desde el momento de la saturación.



  El sistema A y B (características físicas y redes distintas) van a necesitar un equipo en medio que las conecte y que entienda ambas redes, es decir, un router que realiza la traducción.

  Los protocolos hasta el nivel de red son locales (hablan con su sistema adyacente), el resto van a realizar conexión extremo a extremo.

  Los routers solo tienen 3 niveles.

  - **SISTEMAS ADYACENTES:** Sistemas/Equipos conectados a una misma red física.

- **TRANSPORTE (NIVEL 4):** Realiza segmentación de información, es decir, entidades grandes se van a dividir en unidades más pequeñas.

  Se realiza control de errores y control de flujo pero extremo a extremo.

  Las PDU'S de este nivel se llaman **SEGMENTOS** o **DATAGRAMA**.

  Como en el nivel de red se pueden perder paquetes, se necesita un protocolo fiable a nivel de transporte para poder detectarlos.

  Podemos tener dos protocolos diferentes para este nivel:

  - **TCP:** Protocolo fiable pero lento.

  - **UDP:** Protocolo menos fiable (pierde información). Este protocolo se usa cuando perder información no es relevante o cuando estamos usando un protocolo fiable en un nivel superior.

- **SESION (NIVEL 5):** Solo para el modelo OSI de ISO.

  Se encarga de la administración y gestión del dialogo, es decir, si cuando estas enviando datos las conexión se rompe antes de terminar el envío el nivel de sesión evita que se tenga que volver a empezar desde el principio.

- **PRESENTACION (NIVEL 6):** Solo para el modelo OSI de ISO.

  Como los datos que maneja una maquina tienen que entenderse en la maquina destino el nivel de presentación traduce los datos a un lenguaje común a la de transmitirlos (ASN.1) y luego será la maquina destino la que lo traduzca a su propio lenguaje.

- **APLICACION (NIVEL 7):** En TCP/IP engloba los dos niveles anteriores.

  Es el propio proceso de usuario, va a tener tantas entidades como queramos. Cada entidad va a tener su propio protocolo.

  A sus PDU'S se las llama **MENSAJES**.

3.1 Control de Flujo.

- **NIVEL 2:** El control de flujo se realiza sobre la misma red. Se encarga de evitar desbordamiento entre un sistema y el router con el que está conectado.

  El router indica que se pare de enviar información porque se va a saturar y también se encarga de indicar cuándo se puede volver a comenzar a enviar datos de nuevo.
- **NIVEL 4:** Se realiza de extremo a extremo. Va a ser el destino el que se satura no el equipo intermedio y tiene que ser el destino el que se lo tiene que indicar al origen.

  Esto es así por que un router no tiene porque encaminar hacia un único equipo, si que suele encaminar hacia muchos equipos distintos.

3.2 Control de Errores.

En términos generales comprueba que no se pierda información en el encaminamiento de datos.

- **NIVEL 2:** Comprueba que la trama ha llegado correcta, si no ha llegado correctamente se pedirá retransmisión de la trama.

  Se realiza sobre la misma red.
- **NIVEL 4:** El error lo detectara el destino final, pro que al segmentar la información en tramas puede que alguna se pierda. En este caso se pide la retransmisión del segmento entero.

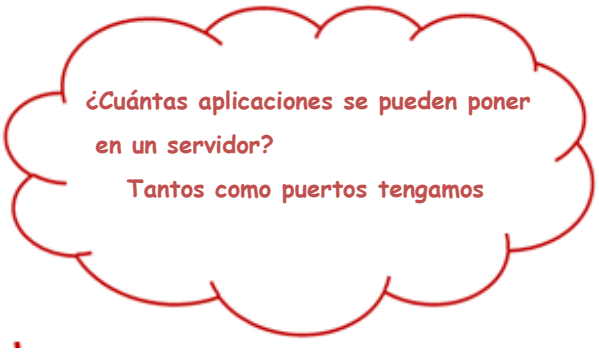
Como los niveles no trabajan con la información de otro nivel el nivel 2 deberá guardar las tramas enviadas hasta que le confirmen que ha llegado correctamente.

Si una red es fiable (Fibra Óptica) no haría falta tener control de errores a nivel 2 porque se perdería mucho tiempo y ancho de banda, pero en este caso si se pierde una trama tendríamos que volver a retransmitir todo el segmento.

Tener un nivel 2 totalmente fiable no asegura que la red sea fiable porque en el nivel 3 se puede perder información, por tanto es obligatorio un nivel 4 fiable (con control de errores).

Cuando una red no es fiable lo lógico es poner en el equipo intermedio un protocolo fiable.

En el caso de usar un protocolo a nivel 4 no fiable, podríamos asegurar fiabilidad utilizando un protocolo fiable en alguno de los niveles superiores.

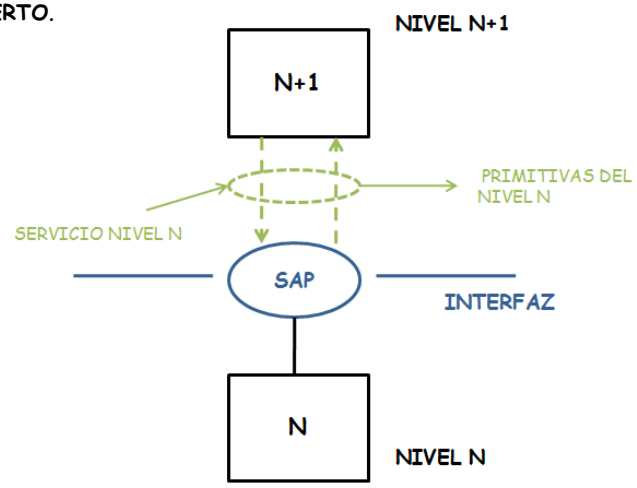


4. Servicios OSI.

- **SERVICIO:** Resultado de efectuar una o más funciones definidas por un protocolo. Un servicio OSI se identifica por un conjunto de primitivas o llamadas a funciones.
- **SAP:** Punto de acceso al servicio. A través de él se comunican entidades.

  Es el punto a través del cual un nivel superior pide un servicio a un nivel inferior y ese nivel le responde diciendo que le ha llegado

  En TCP/IP se le denomina **PUERTO**.



- **INTERFAZ:** Conjunto de funciones que ofrece el nivel inferior al nivel superior para usar los servicios que ofrece.

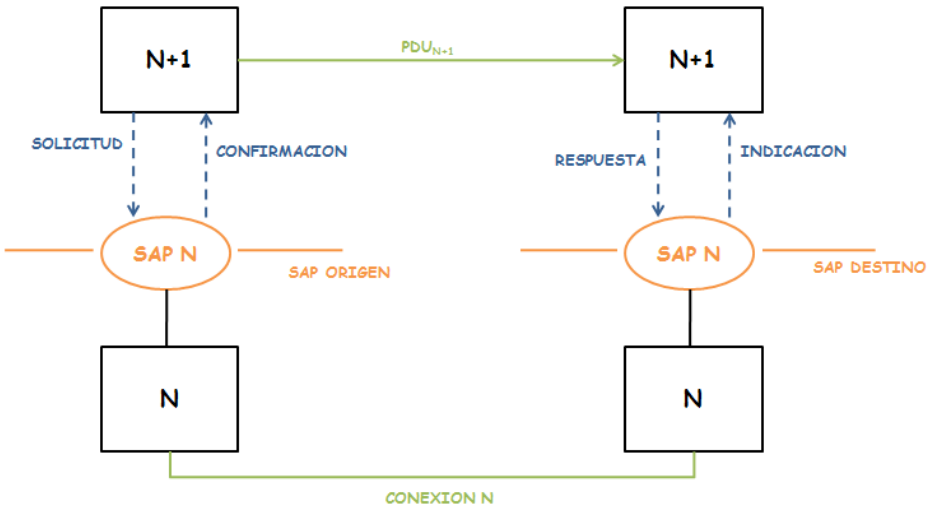
  Dos niveles se comunican a través de su interfaz.

  Un nivel solo se va a poder comunicar con su inmediatamente superior o inferior, el resto serán transparentes.

Hay que distinguir entre: servicio confirmado, servicio no confirmado y servicio fiable.

4.1 Servicio Confirmado.

Una vez que el receptor recibe la PDU (datos) decide mandar una respuesta diciendo que ha recibido el servicio.



Requiere cuatro primitivas:

- **SOLICITUD:** Llamada de la entidad N+1 a la entidad N en el sistema emisor para solicitar un servicio del nivel N.
- **INDICACIÓN:** Llamada de la entidad N a la entidad N+1 en el sistema receptor para indicar a la entidad N+1 que una entidad par ha solicitado un servicio del nivel N para comunicarse con ella.
- **RESPUESTA:** Llamada de la entidad N+1 a la entidad N en el sistema receptor para responder al servicio afirmativamente o abortándolo.

- **CONFIRMACION:** Llamada de la entidad N a la entidad N+1 en el sistema emisor para indicarle que la entidad par quiere confirmar el servicio.

Un servicio confirmado puede no ser fiable ya que la fiabilidad viene determinada en algún nivel inferior. La fiabilidad que da un nivel es independiente del servicio que le da al nivel superior.

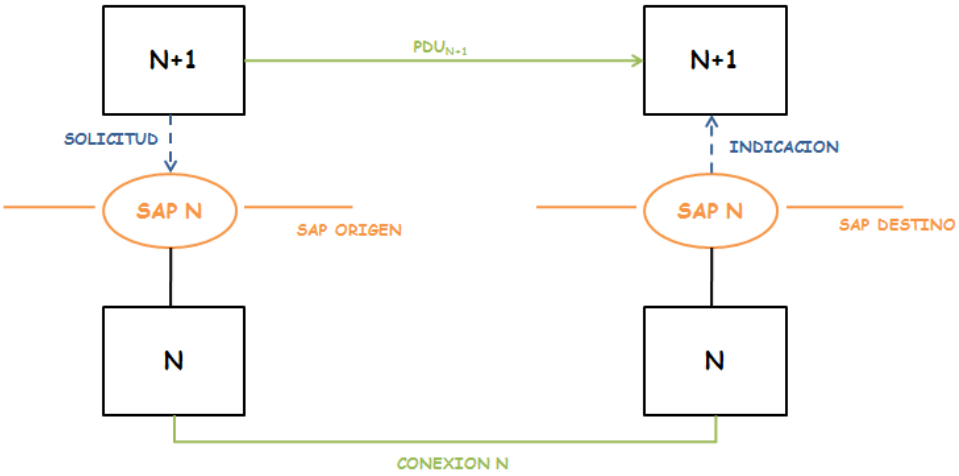
4.2 Servicio No Confirmado.

Su nivel inferior recibe una solicitud de servicio, este manda los datos al receptor y ya está, es decir, no se espera ningún tipo de respuesta de que se ha recibido el servicio.

Solo se necesitan dos primitivas: SOLICITUD e INDICACIÓN

Las primitivas son entre entidades no entre niveles.

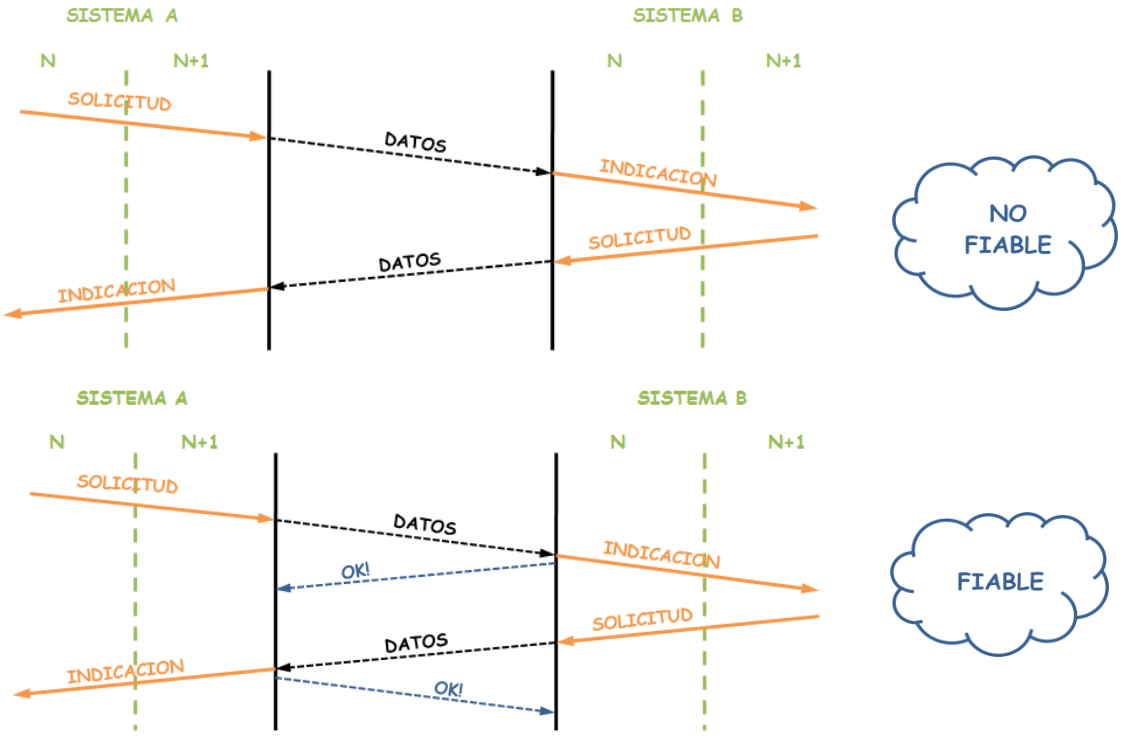
No siempre tiene sentido tener un servicio confirmado, es el caso del envío de datos y la liberación.



4.3 Servicio No Orientado a Conexion.

Son servicios no confirmados, solo se produce la transferencia de datos.

Puede ser o no fiable. Normalmente no son fiables (UDP) solo será fiable si el protocolo del nivel N es fiable.



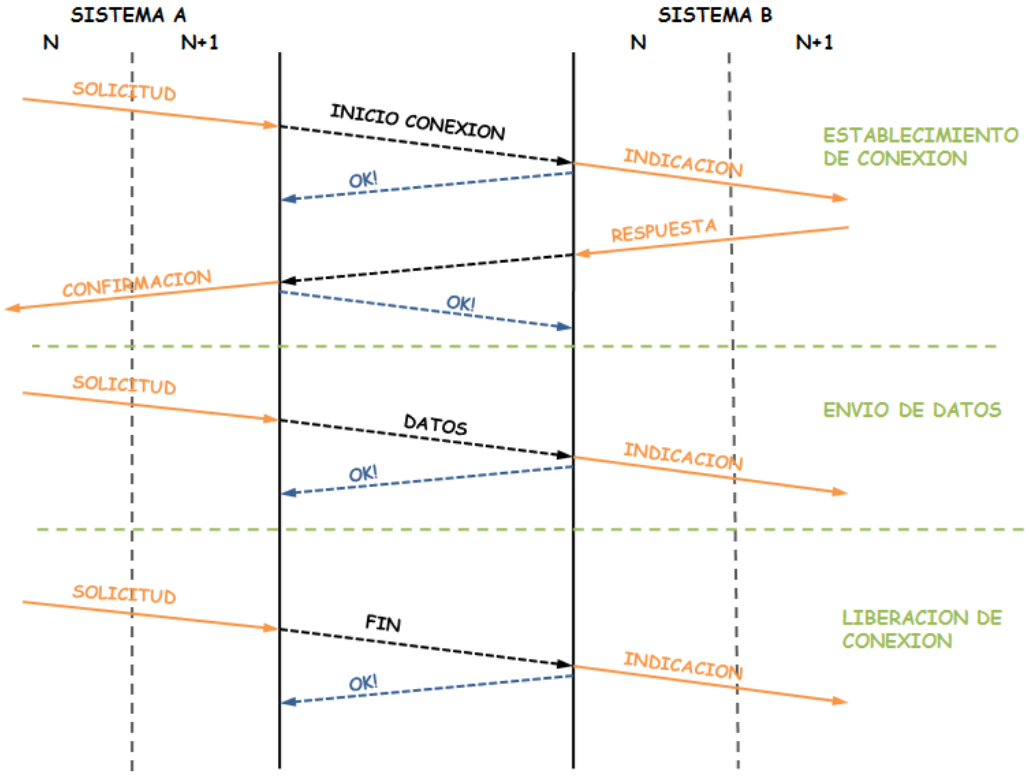
4.4 Servicio Orientado a Conexion.

Es un servicio fiable, como el caso de TCP (Orientado a Conexión)

Tiene tres etapas:

- **SOLICITUD CONEXION:** Esta fase tiene que ser confirmado, porque el sistema B debe indicar al sistema A que se acepta la conexión para comenzar a mandar datos.
- **ENVIO DE DATOS:** Fase no confirmada por que no es necesaria.
- **LIBERACION:** Fase no confirmada, porque si se pierde la orden de liberación es el nivel inferior el que lo localice y solucione, pero el nivel N+1 se despreocupa totalmente.

Independientemente de que una fase sea confirmada o no, todas las etapas son fiables porque el nivel N tiene un protocolo fiable.



La fiabilidad la proporciona el envío del OK!

El OK! Lo envía el nivel N a su otro nivel par para decirle que lo que ha mandado ha llegado bien => Mensaje de confirmación.

- **MENSAJE DE CONFIRMACION:** Mensajes de control que envían niveles inferiores para indicar que la PDU enviada ha llegado bien o no.

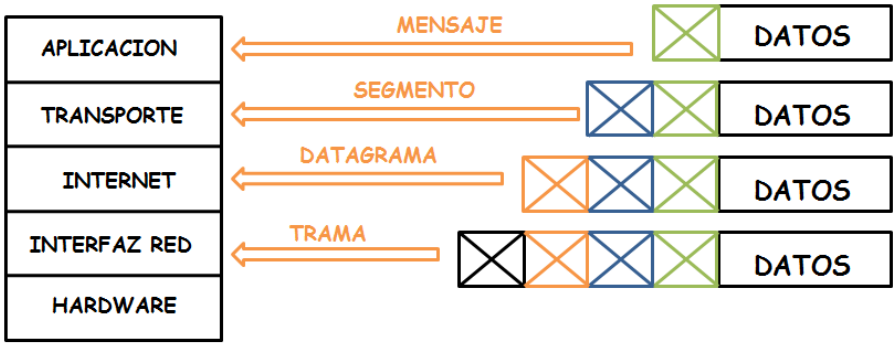
  Si no se mandan mensajes de confirmación, el protocolo no es fiable y no podemos asegurar que la información llegue aunque sea confirmado.

Las primitivas son entre entidades no entre niveles: solicitud va entre el nivel N+1 y su nivel par al igual que la confirmación.

¿Tiene que ser fiable el nivel de RED?

NO (Si lo fuese se tardaría mucho tiempo en conectar y se saturaría la RED).

5. ARQUITECTURA TCP/IP.



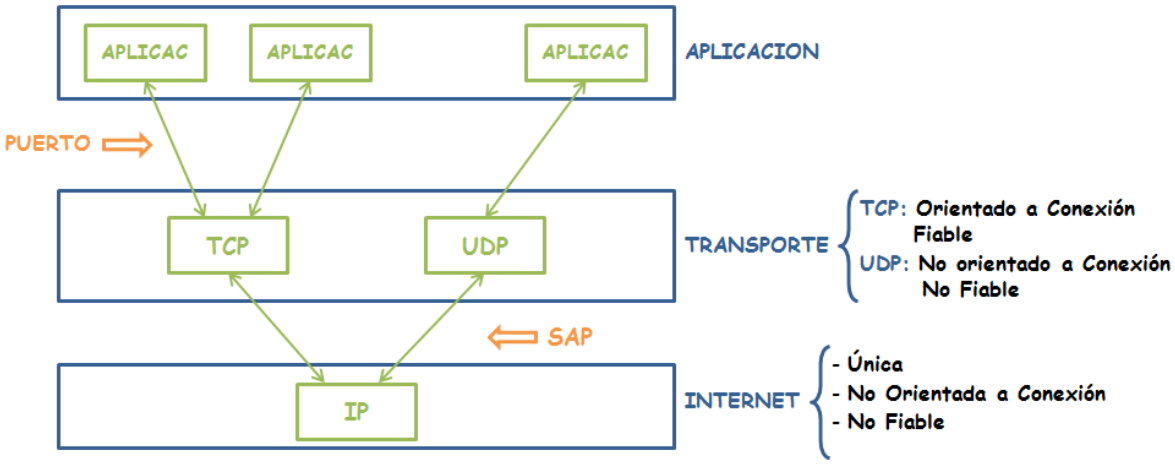
- **DATAGRAMA ≈ PAQUETE:** Unidad atómica de datos que se transmiten.

A nivel internet se encamina la información de manera global usando direccionamiento IP: únicas en todo internet.

A nivel de interfaz de red el encaminamiento es local. Usan direcciones MAC. Las direcciones MAC se pueden repetir y solo tienen sentido dentro de su red local.

La PDU del nivel internet va a contener en su cabecera la IP del destino real y cuando se baja a nivel de interfaz de red le va a añadir a su cabecera la dirección MAC de la red contigua (destino) y la suya (origen).

El datagrama IP no cambia, siempre tiene el origen y el destino real, pero las tramas van a contener los orígenes y destinos parciales (direcciones MAC).



Aunque el protocolo Http no es fiable como usa un puerto TCP, con un protocolo fiable, Http se convierte en un protocolo fiable.

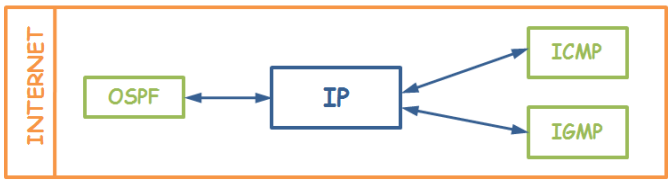
Un puerto TCP y UDP se pueden llamar igual porque lo que les diferencia es el par protocolo-puerto.

- **SAP:** Indica a través de que hueco un nivel pide servicios al nivel superior y este le contesta.

  Se da en todos los niveles y se realiza a través de una interfaz no estandarizada.

5.1 Niveles Inferiores.

- **NIVEL INTERNET:**



En nivel internet puede haber varios protocolos auxiliares (ICMP, IGMP, OSPF).

El único protocolo capaz de dar servicios de encaminamiento a nivel de red es el IP, el resto son accesorios.

- **OSPF:** Sistemas Open shortest Path First

  Protocolos avanzados para routers que usan encaminamiento dinámico, es decir, tablas de rutas dinámicas.

  El encaminamiento se organiza intentando ir por el camino más corto en peso (coste de los enlaces, velocidad…).

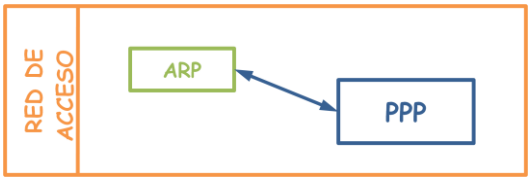
- **ICMP:** Internet Control Message Protocol

  Detecta posibles errores de encaminamiento, para que sean corregidos, pero no los corrige.

  No fiable.

- **IGMP:** Protocolo para encaminamiento entre zonas.

- **NIVEL RED DE ACCESO:**



- **PPP:** Point to Point Protocol

  Protocolo del interfaz de la red de acceso, es decir, es el protocolo del nivel de enlace.

- **ARP:** Address Resolution Protocol

  Solo existe para red Ethernet.

  Traduce la dirección IP del equipo más cercano para llegar al destino final en la MAC destino (del equipo más cercano) para poder enviar las tramas.

  Solo resuelve direcciones IP locales a MAC locales (en su misma red). Usa tablas ARP.

  * TABLA ARP:

DIR IP	MAC ASOCIADA

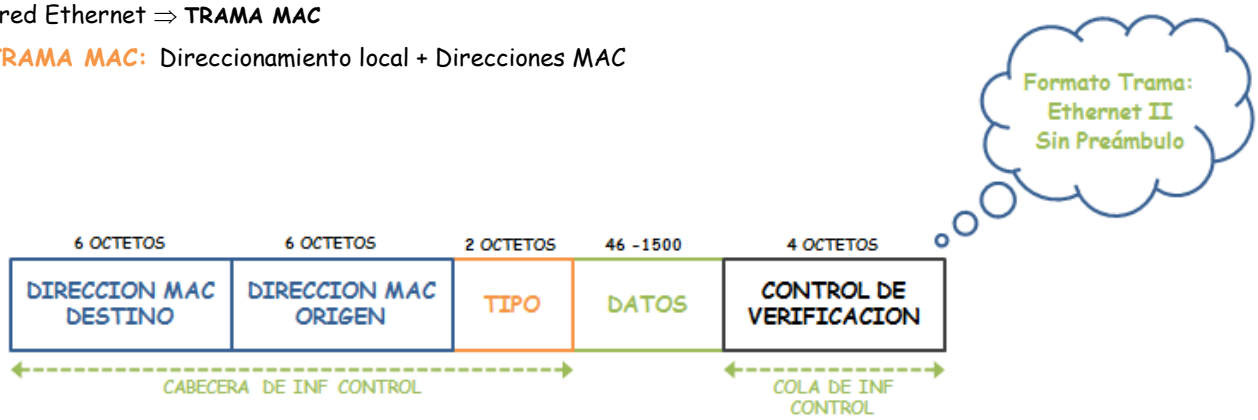
1. Solo tiene datos de su red Local. Los datos serán distintos para otras redes.
2. Solo contiene las entradas estrictamente necesarias para el encaminamiento, son temporales.
3. Se manda un mensaje ARP dentro de una trama que escuchan todos los equipos de la red y el único que localice su IP contestara con otro mensaje ARP.

5.2 Formato de una Trama Mac.

Cada nivel pone la PDU del nivel superior dentro de una trama con su propia cabecera.

A nivel 2 el direccionamiento es a nivel local y el encaminamiento es a través de tramas, si la red a la que se encamina es una red Ethernet ⇒ **TRAMA MAC**

- **TRAMA MAC:** Direccionamiento local + Direcciones MAC

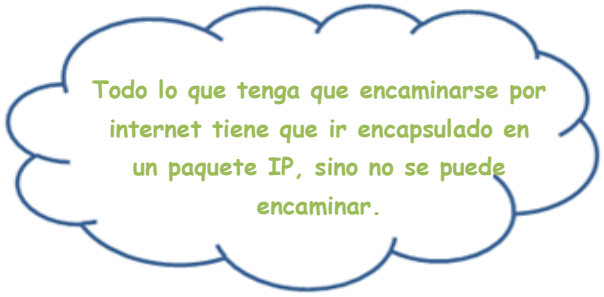


- **DIRECCION MAC DESTINO:** Dirección de la tarjeta de red del equipo destino al que van dirigidos los datos.
- **DIRECCION MAC ORIGEN:** Dirección de la tarjeta de red del equipo origen que transmite la trama.

  Si el destino está dentro de la misma red se envía directamente, resolviendo la dirección MAC asociada a la IP destino.

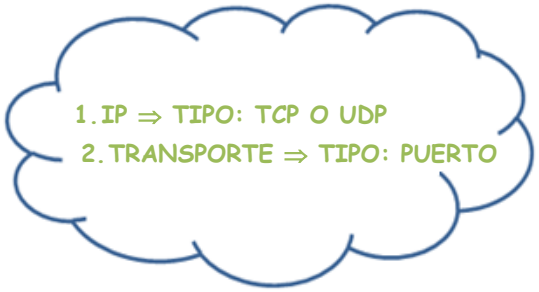
  Si no está, se tendrá que decidir a partir de la tabla de rutas, cual es el siguiente salto para acercarse al destino, que será el router que encamina hacia esa red.

  Una dirección MAC solo tiene sentido dentro de su red local porque mas allá lo resuelve el nivel IP.
- **TIPO:** Identificador del protocolo del nivel superior al que hay que dirigir el contenido de la trama.



1. ICMP es un protocolo que se encapsula dentro de un paquete IP ⇒ Tipo: IP.
2. Un mensaje ARP va metido directamente en trama, no va encapsulado en IP porque al ser local solo encamina desde el router al equipo origen de la red y no debe encaminarse ⇒ Tipo: Protocolo ARP

El SAP (puerto en TCP) debe estar asociado a la cabecera.

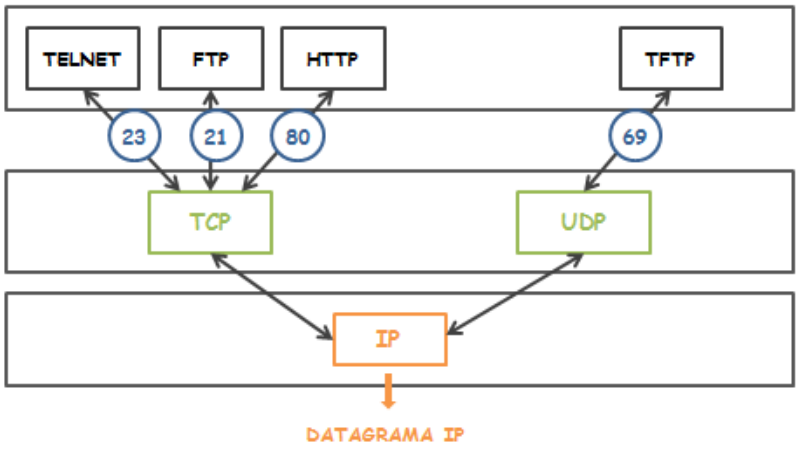


5.3 Puertos.

A nivel de aplicación cada una de las posibles entidades son puertos. La mayoría de aplicación en internet son modelo cliente/servidor.

Cada proceso cliente/servidor viene definido por un numero de puerto.

- **Nº DE PUERTO:** Entero positivo manejado por TCP/UDP para identificar tanto a un cliente como a un servidor.
  - **0 - 1023:** Puertos estándar para servidores. Son fijos.
  - **1024 – 65.535:** Puertos no estándar para servidores y puertos clientes.

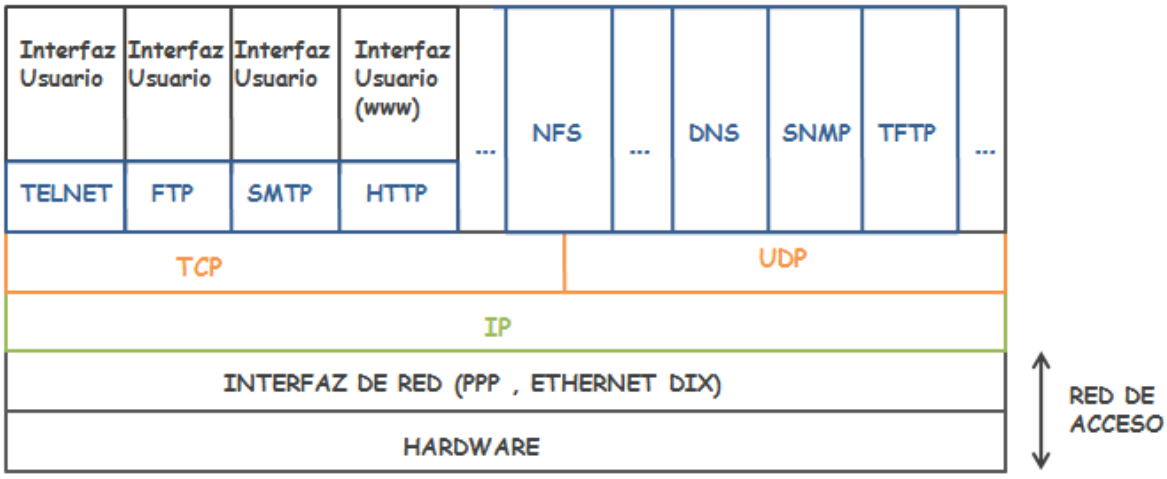


Los puertos estándar evitan tener que saber dónde está el servidor. Un servidor esta sobre un puerto fijo, sino el origen no sabría a donde enviar el datagrama.

El origen no necesita estar identificado con un puerto fijo por que como es el que inicia la comunicación solo manda datos.

Varios clientes de una misma máquina pueden interactuar con un servidor igual o distinto.

5.4 Protocolos Más Significativos.



- **TELNET:** Aplicación que permite conectarnos a otro ordenador remoto a través de la red, manejándolo como si estuviéramos delante.
- **TFTP:** Protocolo de gestión de ficheros
- **FTP:** Protocolo de transferencia de archivos entre sistemas conectados a una red TCP. Basado en arquitectura cliente- servidor.
- **HTTP:** Protocolo de transferencia de hipertexto. Protocolo sin estado, es decir, no guarda información de conexiones anteriores a internet.
- **DNS:** Sistema de nombres de dominio que permite traducir el nombre del dominio a dirección IP y viceversa.
- **NFS:** Sistema de archivos de red que posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos
- **SNMP:** Protocolo simple de gestión de red (de distintos ordenadores de una red). Permite hacer cambios en el ordenador.
- **SMTP:** Protocolo simple de transferencia de correo electrónico.

.